PERFORMANCE WORK STATEMENT (PWS)

INFORMATION TECHNOLOGY (IT) SUPPORT SERVICES
FOR
DLA INFORMATION OPERATIONS

SECTION 1 INTRODUCTION

A. The Defense Logistics Agency (DLA) is a United States (U.S.) Department of Defense (DoD) agency that provides worldwide logistics support for the missions of the Military Departments and the Unified Combatant Commands under conditions of peace and war.

B. DLA Information Operations has a requirement for contracted IT support services for on-site hardware, software, and technical support at the designated place of performance (*see section 2.2.1 – Place of Performance*). IT support services are required to augment existing Government IT support personnel.

C. The primary objective is to ensure that all IT equipment, to include network hardware, server hardware, workstations, printers, portable computers, network infrastructure (cabling), and miscellaneous IT equipment, is functioning at all times to support mission requirements. IT support services shall be provided to users when working at their primary duty location, when working from an alternate site, and/or when working in a temporary duty (TDY) status away from primary duty location.

D. Installation, maintenance, and troubleshooting support is required for all IT and IT related pieces of equipment to include workstations/laptops, printers and peripherals, such as, CD/DVD readers /writers, controllers, antennas, Ethernet cards, switches, routers, hubs, modems, media converters, monitors, keyboards, print servers, plotters, scanners, wireless bridges, RF network controllers, RF access points, RF handheld units, RF vehicle-mounted units, digital cameras, and LCD Boards.

E. Work environment is in typical office settings, a server room, wiring closets and multiple warehouse production buildings. Work may require utilization of man-lifts for access to IT equipment mounted at higher elevations. Work may be dirty in nature for warehouses with limited environmental controls for temperature and humidity.

Est. # Users	Est. # Buildings	Est. Distance	Est. Equipment Elevation	Est. # Workstations/ Laptops	Est. # Printers	Est. # Peripherals
838	29	45 mile radius	Up to 40 feet	880	769	2,800

SECTION 2 GENERAL CONDITIONS AND REQUIREMENTS

A. This Section provides general information relating to the conditions of operation and general requirements relating to the IT support services required.

2.1 SCOPE OF WORK

A. The Contractor shall provide all personnel, equipment, supplies, facilities, road vehicles, transportation, tools, materials, cell phones, supervision, and other items/services (other than those designated as Government-furnished per Section 4, *Government-Furnished Property (GFP), Systems, Training and Support Services*) necessary to perform IT Support Services as defined in this PWS.

B. IT Support Services required includes on-site support for problem reporting and resolution for end users and the overall computing environment. All work and trouble requests shall be identified to the contractor via the Incident and Asset Management Tracking System (*listed in Section 2.3 – Computing Environment*) as well as problems received (or referred) via phone, email or direct contact. The Contractor shall be responsible for communicating via written trouble ticket or work order for all repairs, installations, troubleshooting, and for ensuring response times are met.

	Required Response Times			
Estimated Total Incidents per Month for all four (4) priorities.	**Priority 1**	**Priority 2**	**Priority 3**	**Priority 4**
550-750	< 1 Hour	< 3 Hours	< 24 Hours	< 72 Hours

C. Completed trouble tickets and work orders shall be closed out in the Government's Incident and Asset Management Tracking System within twenty four (24) hours after completion of work.

D. This is a non-personal services contract to provide information technology support services. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn, is responsible to the Government. The Government and the Contractor understand that the services to be provided under this contract by the Contractor are non-personal services and that no employer-employee relationship exists between the Government and the Contractor. The Government may provide technical direction which will assist the Contractor in accomplishing the PWS; however, the Government will not control the methods used by the Contractor to perform the service requirements set forth in the PWS.

2.2 GENERAL OPERATING CONDITIONS

A. This Section provides general information relating to the conditions of operation and general requirements relating to the IT support services required.

2.2.1 PLACE OF PERFORMANCE, DUTY HOURS AND ACCESS TO THE HOST INSTALLATION

A. Work will be accomplished primarily at DLA locations in Norfolk, VA 23512, to include regional locations.

B. The Contractor shall perform services required under this PWS in accordance with the Duty Hours identified in the PWS except Federal holidays and base closures.

C. The Contractor shall provide occasional on-call support for End User support and Network administration support. On call support is anticipated to occur no more than six (6) times per year for End User support and no more than eight (8) times per year for Network administration support.

	Naval Station, Norfolk, VA	Norfolk Naval Shipyard (NNSY), Portsmouth, VA	Naval Amphibious Base, Little Creek, VA	FISC Cheatham Annex, Williamsburg, VA
Est. # Users	522	276	10	30
On-Site or Remote Support	On-Site	On-Site	Remote	Remote
Duty Hours	0630 – 1800 Monday - Friday	0630 – 1800 Monday - Friday	0630 – 1800 Monday - Friday	0630 – 1800 Monday - Friday
Est. Travel Time	N/A	N/A	15 minutes	60 minutes
Est. frequency of on-site support	Daily	Daily	Once per month	Once per month

D. Travel between sites during regular duty hours is considered inherent to the tasks detailed in the PWS and will not be reimbursed.

E. Other travel costs will be paid for in accordance with the Joint Travel Regulations.

F. Due to changing traffic requirements brought on by construction, changing missions, and security concerns within the host installation, access to the host installation is subject to change, sometimes with little or no warning. Inbound and outbound traffic restrictions exist.

2.2.2 PERIOD OF PERFORMANCE

A. The period of performance for this contract action will be for a one year base period with four (4) one (1) year options.

2.2.3 FEDERAL HOLIDAYS

A. Federal holidays generally observed by government personnel include:

Observed Federal Holidays	
New Year's Day	Martin Luther King Day
Presidents Day	Memorial Day
Independence Day	Labor Day
Columbus Day	Veterans Day
Thanksgiving Day	Christmas Day

B. In the event an Executive Order issued by the President of the United States declares Agencies of the Federal Government closed for a regularly scheduled workday, the Contracting Officer (KO) or

Contracting Officer's Representative (COR) will determine and advise the Contractor on whether services are required for that day.

2.3 COMPUTING ENVIRONMENT (CE) AND OPERATING SYSTEMS

A. The following list identifies the computing environment (CE), operating systems and data systems for which the Contractor shall be required to provide support (or use) which includes but is not limited to:

- Microsoft Windows7 Enterprise workstations, Windows 2008 enterprise servers.
- Cisco and Enterasys networking equipment (routers, switches and access points).
- Various models of Kyocera, Intermec and Printronix printers.
- Various models of Dell servers, desktops, laptops, monitors, keyboards and mice.
- Psion/Teklogix Radio Frequency (RF) handhelds and mobile mounted terminals.
- BMC/Remedy Incident and Asset Management System

2.4 PERSONNEL QUALIFICATIONS AND CERTIFICATIONS

A. Contractor personnel must be proficient in reading and capable of communicating effectively in English.

B. Contractor personnel performing tasks under this PWS shall have appropriate level DoD 8570 IT level certifications for Information Assurance Technical (IAT) and appropriate level DLA approved Computing Environment (CE) certification(s) as identified in Table 2.4.1, *IAT and CE Certification Requirements*.

Table 2.4.1, *IAT and CE Certification Requirements*

Approving Authority	Functional/ Support Type	Certification	Requirement
DoD Approved IAT Level II Baseline Certifications	End-User Support/ Desktop Support and/or Network Administrator	GSEC, SCNP, SSCP, or Security+CE	Personnel performing work must have and maintain at least (1) certification at the IAT II or IAT III Level
DoD Approved IAT Level III Baseline Certifications	End-User Support/ Desktop Support and/or Network Administrator	CISA, GCIH, GSE, SCNA, and CISSP	
DLA Approved CE Certifications	End-User Support/ Desktop Support	MCDST, MCITP EDST, MCITP EDA, MCM, MCSA, MCSE, Windows 7(passing exams 70-680 or 70-682), and Windows XP (passing exams 70-270, 70-271 and/or 70-272).	Personnel performing work must have and maintain at least (1) CE from the list. CE requirements depend on the **Functional/ Support Type** being performed.
	Network Support/ Administrator	CCSE NGX, CCNA, CCNP, CCIE, CCSP, SCNA, CCSE NGX Plus NG with AI, CCMSE NG with AI, CSMSE NG with AI Plus VSX, NSA, ESE, and ECIE-C.	

NOTE: Refer to Section 3.2 for Acronym Definitions

* All tasks performed under this PWS are categorized under Information Assurance Technical (IAT) Level II positions as outlined in DoD 8570.01-M. No waivers or extensions will be provided for mandatory DoD IA or DLA CE certification requirements. Contractor personnel who fail to maintain the required certifications are subject to KO directed removal for performance under Section 2.5 of the PWS.

Network Administrator – Primary responsibilities include the setup and administration of Operating Systems, servers, workstations, laptops, file servers, firewalls, related telecommunications and network software and hardware. Optimizes system operations and resource utilization and performs system capacity analysis and planning.

End-User Support – Experience installing PC software and hardware in network environment. Troubleshoots and resolves problems with networked PCs and other networked hardware and software.

C. The Contractor shall implement a continuing recruiting program such that the Contractor can respond to urgent and phased surge and mobilization requirements. Personnel assigned to or utilized by the Contractor in the performance of this contract shall possess the qualifications and skills set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. If the KO or COR questions the qualifications or competence of any person performing under the contract, the burden of proof that the person is qualified as prescribed herein shall be upon the Contractor.

D. The Contractor shall be responsible for obtaining all necessary licenses and certifications and for complying with all applicable Federal, State, and local laws. The Contractor shall maintain updated copies of any applicable licenses and certifications for all employees and provide copies to the COR.

E. Contractor personnel may be required to access IT equipment stored in a warehouse environment, Contractor personnel shall possess the knowledge and skills (to include licensing and certifications) necessary to operate various types of material handling equipment (MHE) , i.e., forklifts, scissor and boom lifts, dollies, pallet jacks, golf carts, mini-trucks/vans. Contractor personnel that operate motor vehicles shall maintain a valid state driver's license with all class and commodity endorsements required by Public Law 99-570 and state law for the type of vehicle operated.

2.4.1 MANAGEMENTPERSONNEL (KEY PERSONNEL)

A. Team Lead. The Contractor shall appoint a Team Lead who shall be on-site at the place of performance designated in paragraph 2.2.1. The Team Lead shall be available via telephone or email during the normal hours set forth in paragraph 2.2.1 for emergency problem resolution. The Contractor shall determine the labor category for the Team Lead based on the Contractor's proposed staffing plan.

B. Team Lead Skills:

1. Possess the basic knowledge and skills required to plan, control, and manage contract performance. The team lead shall be responsible for the successful completion of the work and shall be qualified to be the Contractor's on-site supervisor and POC for the Contracting Officer or designee.

2. Ability to provide overall supervision for Contractor employees to include, but not limited to, planning and managing the project professionally, ensuring that work is scheduled properly to obtain maximum use of resources; ensuring that accurate and timely reports are provided.

3. Possess the authority to resolve problems, allocate resources, manage personnel, and monitor operation performance to ensure complete satisfaction.

C. The Contractor shall provide the name, telephone number (to include mobile telephone and pager, as applicable) and e-mail address of the Team Lead in writing. In the event of the replacement of the Team Lead, the Contractor shall notify the KO or COR, in writing, of such replacement. The name, telephone number (to include mobile telephone and pager, as applicable) and e-mail address of the replacement Team Lead shall be provided to the KO or COR at least 15 calendar days prior to a planned replacement and within 24 hours following an unplanned replacement.

2.4.2 TECHNICAL PERSONNEL

A. Personnel utilized by the Contractor in the performance of work required under this contract shall possess the certifications, qualifications and skills set forth below.

1. End User Support Skills:

(a) Network+ certification or any approved certification demonstrating working knowledge and understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) networked environment.
(b) Security+ certification or any approved certification demonstrating working knowledge and understanding of applying basic security principles to the computing environment (CE).
(c) Certified in a currently supported Microsoft Windows desktop operating system(s) with working knowledge of applications, System Center Configuration Manager, Microsoft's Active Directory (AD) as related to integration of desktop systems into AD, and all aspects of Windows security to include any subsequent software releases/upgrades.
(d) Ability to troubleshoot hardware and software problems related to desktop computers, Print servers, scanners, printers, PDAs (Blackberries), desktop video/video teleconference systems, and peripherals (zip drives, external zips, scanners, etc.).
(e) Ability to provide hardware maintenance such as board replacement, cable switching, communications assistance, and hardware installation and replacement.
(f) Knowledge of industry standard Incident Ticket Tracking systems for inputting incident tickets and creating work orders.
(g) Demonstrated knowledge and accomplishment in analyzing, diagnosing and recommending solutions for hardware and software problems.
(h) Knowledge of IBM's Customer Information Control System (CICS) and Virtual Telecommunications Access Method (VTAM) Printer Support System (VPS) to restart printers and printer output.
(i) Demonstrated ability with installation, configuration, and the ability to learn DLA-unique applications and programs.
(j) Demonstrated understanding of End-User Radio Frequency (RF) hardware/software devices and the ability to perform minor repairs or configurations.
(k) Ability to troubleshoot Microsoft products including, but not limited to, Windows, Office; including all aspects of Windows security and Microsoft desktop products
(l) Understanding and knowledge of Windows XP and MS Office; to include ability to install any subsequent releases/upgrades.
(m) Expertise to install and support workstation hardware and software, to include depot-unique items as instructed by the Government.

2. Network Administration Support Skills:

(a) Network+ certification or any approved certification demonstrating working knowledge and understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) networked environment.
(b) Security+ certification or any approved certification demonstrating working knowledge and understanding of applying basic security principles to the network environment (NE).
(c) Certified in network operating system/software to include ability to install any subsequent software releases/upgrades.
(d) Knowledge of network sniffer technologies and/or other network management software.
(e) Knowledge of Enterasys and/or Cisco network hardware and software.
(f) Knowledge of network troubleshooting/administration, network switching and network equipment, including routing and switching.
(g) Knowledge of technology network appliance and console software and network design.
(h) Understanding of fiber optic cable use, maintenance and fabrication for building infrastructure; and IEEE 802.1x networking standards.
(i) Capability to configure and troubleshoot network equipment, and identify and resolve hardware/software/network malfunctions.
(j) Knowledge of Radio Frequency (RF) hardware, software and infrastructure and ability to perform minor repairs or configurations.
(k) Ability to troubleshoot Enterasys and/or Cisco products, including all aspects of security.
(l) Expertise to install and support workstation hardware and software, to include depot-unique items.
(m) Ability to troubleshoot, repair/install interior building network cable infrastructure.

2.5 SECURITY

A. The Homeland Security Presidential Directive 12 (HSPD-12) dated 27 August 2004 has established criteria for contractors who require a Common Access Card (CAC) for either physical access to a U.S. Government controlled installation or access to government information technology (IT) systems. The Government requires Personnel Security Investigations (PSI) to establish that applicants or incumbents either employed by the Government or working for the Government under contract are suitable for the job and/or are eligible for a public trust position. These positions have been designated as IT Level II and require a Secret clearance. Contractors shall be required to provide appropriate background investigation for IT-II with Secret clearance as required in accordance with DoD 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM) and DoD 5200.2-R. The appropriate background investigation for IT-II with Secret clearance is a National Agency Check with Local Agency Check and Credit Check (NACLC). The Contractor shall forward their employee clearance information to**:**

DLA Distribution at Norfolk
ATTN: Security Officer
1968 Gilbert Street
Norfolk, VA 23512

B. All personnel employed by the Contractor in the performance of this contract, or any representative of the Contractor entering a U.S. Government installation, shall abide by all security regulations and policies of the installation including access badges, parking, access to controlled or restricted areas, classified information, controlled unclassified information, data and IT resources.

C. DLA reserves the right to direct the removal of an employee, whose actions, while assigned to this contract, clearly conflict with the interests of the Government, regardless of prior clearance or adjudication status. DLA also reserves the right to direct the removal of an employee for misconduct, security violations, or performance reasons. The reason for removal shall be fully documented in writing by the Contracting Officer. When and if such removal occurs, the contractor shall assign qualified personnel to any vacancy(s) thus created within 10 working days. This action does not relieve the contractor from total performance of the contract tasks specified herein.

D. Contractor shall return all government issued identification, access badges, and vehicle passes to the KO or COR upon termination of service.

E. The provisions outlined above apply to the prime contractor and any subcontractors the prime contractor may employ during the course of this contract. No contractor personnel performing sensitive duties shall be allowed to commence work on this effort until his or her trustworthiness has been favorably adjudicated.

2.5.1 DOD COMMON ACCESS CARD (CAC)/ACCESS IDENTIFICATION BADGE (ID BADGE)/ELECTRONIC KEY CARD

A. Every Contractor employee shall obtain and possess a DoD Common Access Card (CAC) and an Access ID Badge as required. Upon favorable review and initiation of the PSI to establish the suitability of an employee for the job and the approval for temporary Automated Information System (AIS) access pending final adjudication of the PSI, the Contractor shall submit to the KO a request for the DoD CAC and ID Badge.

B. The Contractor shall safeguard CAC and ID Badges furnished to them. Contractor employees shall not share CAC and ID Badges. Each Contractor employee shall wear the ID Badge conspicuously on his or her outer clothing above the waist at all times while working on the installation. Personnel may be challenged and removed from the work area or denied access to the host installation if the ID Badge is not worn.

C. In the event that a Contractor employee damages or loses his or her CAC and ID Badge, the Contractor shall report the lost or damaged CAC and ID Badge within two (2) working hours of damage or loss to the KO or COR who will arrange for a replacement CAC or ID Badge. The Government will issue the Contractor employee a temporary ID Badge to be used for an eight to ten (8-10) working day waiting period until a new permanent ID Badge is issued. The Contractor shall return all government-furnished CAC or ID Badges to the Government either within one (1) working day of the completion of the contract or upon termination of an individual's employment, whichever comes first. Contractor personnel failing to return their Government CAC or ID Badge are subject to criminal charges under USC Title 18, Chapter 1, Section 499 and 701.

D. The KO or COR will provide and maintain electronic key cards for the security access system. The electronic key card allows access to specific controlled areas of the facilities. The KO, COR or designee will approve and provide the electronic key cards to the Contractor for access to the facilities.

2.5.2 INFORMATION SYSTEM SECURITY

A. Upon favorable review and initiation of the PSI to establish the suitability of an employee for the job and the approval for temporary AIS access pending final adjudication, but not less than fourteen (14) working days prior to the employee's start date, the Contractor shall request Information Technology

(IT) eligibility for an employee requiring access and passwords to the government-furnished data systems. All positions involving computer activities require a minimum IT II category eligibility. The Contractor shall submit a Contractor Investigative Request (CIR) and a DD Form 2875 for temporary IT II eligibility, with final eligibility contingent upon receiving a favorably adjudicated background investigation.

B. All Contractor personnel provided with access to government-furnished computers and systems shall observe local AIS security policies and procedures as provided by the KO or COR. The Contractor shall notify the KO or COR within 12 hours when, for reasons of personnel resignation, reassignment, termination, or completion of portions of the contract, Contractor personnel no longer require access to government systems.

C. The Contractor shall observe all copyright agreements. In the interest of protecting government systems from computer viruses, the Contractor shall not use public domain software nor shall Contractor personnel download software from public bulletin boards or Internet websites. The Contractor shall use only commercial off-the-shelf (COTS), Contractor-developed, or government-furnished software in performance of the contract requirements. Should the introduction of a computer virus or malicious destruction of computer software, stored information, or hardware result from the use of public domain software or from software taken from a public bulletin board or Internet website, the Contractor shall be required to repair the damage and incur all costs at no expense to the Government and without impact on delivery schedules.

2.5.3 CONTACT OF A SUSPICIOUS NATURE

A. Contractor personnel who have been contacted under suspicious circumstances shall report that contact immediately, either verbally or in writing, to their supervisor who shall report it within two (2) hours to the KO or COR for action. Key contacts for reporting purposes are defined as:

1. Contact with an individual (regardless of nationality) that suggests to the Contractor employee that an intelligence gathering or terrorist organization may have targeted him or her for possible intelligence exploitation.
2. A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or unclassified sensitive information.
3. Contact with a known or suspected intelligence officer from any country.
4. Contact with a foreign diplomatic establishment, whether in the U.S. or abroad, for personal or official reasons. Certain Contractor personnel in positions designated as “sensitive” by the Government may also be required to inform their chain of command in advance of the nature and reason for contacting a foreign diplomatic establishment or travel to countries on the State Department list whose interests may be adverse to the United States.

B. Additionally, Contractor personnel who have information about activities pertaining to espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, unauthorized release of classified or unclassified controlled information, or unauthorized intrusions into automated information systems shall report that information immediately to the KO or COR for action.

2.5.4 SAFEGUARDING INFORMATION

A. The Contractor shall not allow access or disclosure of information regarding the operations of DLA to any government agency, non-government agency, or individual unless specifically authorized by the KO or COR. The Contractor shall provide documents and files requested by such parties to the KO or COR within one hour of receipt of the authorized request.

B. The Contractor may be required to access data and information that is proprietary to a government agency or contractor or that is of such nature that its dissemination and use other than as specified in this contract would be adverse to the interests of the Government or others. The Contractor and its personnel shall not divulge or release data or information developed or obtained under performance of this contract except to government personnel who are authorized to receive the information or upon written approval of the KO or COR. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend other than as specified in this contract.

C. Disclosure of information regarding operations and services of DLA to persons not entitled to receive it, or failure to safeguard any classified information that may come into the Contractor's control in connection with work under this contract, may subject the Contractor, its agent, or its employees to criminal liability under USC Title 18, Crimes and Criminal Procedure, Part I, Crimes, Chapter 37, Espionage and Censorship, Sections 793, Gathering, Transmitting or Losing Defense Information, and Section 798, Disclosure of Classified Information. Neither the Contractor nor its employees shall disclose or cause to be disseminated any information concerning the operations of the activity which could result in, or increase the likelihood of, the possibility of a breach of DLA's security or interrupt the continuity of DLA's operation.

2.5.5 POTENTIAL OPERATIONAL CONSTRAINTS

A. Force Protection Conditions (FPCONs) may affect access to the host installations and DLA facilities. The FPCON is established by the host installation or higher national command authorities, and the Installation Commander is responsible for implementing the proper response to progressive levels of terrorist threats. FPCONs are normally displayed at most entrance gates, building entrances and office entrances. The Contractor shall adhere to and operate IAW any restrictions imposed as a result of a FPCON. Measures implemented under the various levels of terrorist threat may impact the Contractor's normal operational approach to IT support services. The Contractor shall ensure that IT support services are sustained during heightened security measures.

2.6 ENVIRONMENTAL, SAFETY, AND OCCUPATIONAL HEALTH (ESOH)

A. The Contractor shall formulate and maintain a written safety and health plan and make available to the Government upon request. The written plan shall include the details of the Contractor's responsibilities, method of program implementation, and how hazards and deficiencies shall be identified and corrected. It shall detail Contractor personnel responsibilities for: protection of Government property and safety of others, personnel responsibilities for reporting all mishaps, and establish procedures for reporting to correcting unsafe conditions, hazards, or practices. The Contractor shall have a central POC for safety and health related issues. The POC shall be identified in writing to the KO or COR.

B. The Contractor shall ensure employees have safety education when engaged in activities involving Government facilities, personnel, or equipment.

C. The Contractor shall notify the KO or COR immediately after the occurrence of all accidents and incidents resulting in either personal injury, loss of life, impact to the environment or property damage to a government facility or equipment. The Contractor shall submit a completed copy of

DLA Form 1591 and supplemental information within four (4) working days of the accident or incidents.

D. The Contractor shall require their personnel to wear personal protection equipment (PPE) (i.e. safety shoes or safety boots, hearing protection, eye protection, gloves, safety harnesses) during the performance of this contract in accordance with OSHA standards. The Government will not be responsible for furnishing or paying for the cost of PPE.

E. The Contractor shall comply with all federal, state, and local environmental laws to include but not limited to Resource Conservation and Recovery Act (RCRA), Safe Water Drinking Act (SWDA), the Clean Air Act (CAA), and Federal Facilities Compliance Act (FFCA).

2.7 PHASE-IN PERIOD

A. The phase-in period shall begin at the effective date of the contract and shall not exceed one (1) month, at which time full performance shall commence.

B. Within five (5) calendar days from the effective date of contract award, the Contractor shall complete all required hiring actions for the Team Lead. Within 20 calendar days of the effective date of the contract, the contractor shall complete any associated training and certification requirements. The Contractor shall ensure that all new employees are trained and ready to begin working on the first day of full performance.

2.8 PREPAREDNESS EXERCISES

A. As directed by the KO or COR, the Contractor shall participate in preparedness exercises relating to security disaster preparedness and response, wartime response, and emergency and environmental and similar preparedness exercises.

B. The Contractor shall participate in emergency and recall notification and personnel accountability exercises. The Contractor shall establish emergency notification and recall and personnel accountability procedures in accordance with DoDI 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters, and test those procedures twice a year when directed by the KO or COR. During the exercise, the Contractor shall determine the status and whereabouts of assigned personnel, report the status of each Contractor employee to the KO or COR within established timelines, and continue to report periodic status until further direction by the KO or COR. The Contractor shall follow their personnel accountability procedures in the event of a real emergency as directed by the KO or COR.

2.9 CERTIFICATION AND ACCEPTANCE

A. The KO or COR is designated as the point of final inspection and acceptance by the Government of all items and services required by the contract.

2.10 MAN HOUR REPORTING

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Defense Logistics Agency via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs

October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at help desk at: http://www.ecmra.mil.

SECTION 3 DEFINITIONS AND ACRONYMS

3.1 DOD DICTIONARY

A. The DoD Dictionary of definitions and terms is available on the Internet at: http://www.dtic.mil/doctrine/dod_dictionary/.

3.2 ACRONYMS

A. Following are acronyms from Table 2.4.1, *IAT and CE Certification Requirements*:

SYMBOL	DEFINITION
GIAC	Global Information Assurance Certification
GSEC	GIAC Security Essentials Certification
SCCP	Systems Security Certified Practitioner
CISA	Certified Information Systems Auditor
GSE	GIAC Security Expert
GCIH	GIAC Certified Incident Handler
CISSP	Certified Information Systems Security Professional
MCDST	Microsoft Certified Desktop Support Technician
MCITP	Microsoft Certified IT Professional
EDST	Enterprise Desktop Support Technician
EDA	Enterprise Desktop Administrator
MCM	Microsoft Certified Master
MCSA	Microsoft Certified Solutions Associate
MCSE	Microsoft Certified Solutions Expert
MCTS	Microsoft Certified Technology Specialist
MCP	Microsoft Certified Professional
CCNA	CISCO Certified Network Associate
CCIE	CISCO Certified Internetwork Expert

SYMBOL	DEFINITION
ESE	Enterasys System Engineer
SCNA	Sun Solaris Certified Network Administrator
CCNP	CISCO Certified Network Professional
CCSP	CISCO Certified Security Professional
NSA	EC-Council Network Security Administrator
ECIE-C	Enterasys Certified Internetworking Engineer for Infrastructure

SECTION 4 GOVERNMENT-FURNISHED PROPERTY (GFP), SYSTEMS, TRAINING AND SUPPORT SERVICES

4.1 GENERAL INFORMATION

A. The Government will provide access to resources and information to include Government transactional data systems required in the performance of this PWS.

B. The Government will furnish on-site training for unique Government systems (GOTS) in performance of this PWS.

C. The Government may require Contractor personnel attend mandatory on-site or off-site training on DLA's IT equipment, systems and/or network environment. The Government will be responsible for instructor costs associated with this Government-furnished training. The Government will reimburse the Contractor for travel costs allowed under FAR Part 31.205-46, *Travel Costs* for attending Government-furnished off-site training.

D. The Government will provide on-site office space with furniture, to include computer and network printer, office supplies and desk telephone.

E. At no cost to the Contractor, the Government will furnish the services to be used exclusively to perform the requirements of this contract that include custodial services, refuse and recycling collection, government forms, emergency medical services, police and fire protection, telephone and utilities.

F. When tasks to be performed and/or areas to be reached require the use of MHE, i.e., forklifts, man lifts, etc., the Government will schedule equipment for Contractor use at no cost to the Contractor. The Government will provide all materials, parts, equipment and supplies that Contractor personnel will need to perform this requirement. This does not include contractor furnished motor vehicles (i.e. cars, vans and/or trucks).

SECTION 5 CONTRACTOR RESPONSIBILITY FOR EQUIPMENT AND TRAINING

5.1 CONTRACTOR-FURNISHED TRAINING

A. The Contractor shall provide training (not designated as Government furnished) which may be required for Contractor personnel to comply with the contract requirements. The Contractor shall be responsible for all costs associated with this training. The Contractor shall maintain copies of training records, designation letters and certificates on site and make them available for the KO or COR to review upon request. The training records shall include, at a minimum, the name of the employee, the

name of the course, the source of the training, a description of the training provided and the date the employee successfully completed the training. The Contractor shall furnish the following training:

1. **INFORMATION ASSURANCE (IAT) TECHNICAL TRAINING:**
Contractor personnel performing tasks associated with this PWS that will be performing an IA function shall be trained and certified in accordance with DoD Directive 8570.1 *Information Assurance Training, Certification, and Workforce Management* and DoD 8570.1-M *Information Assurance Workforce Improvement Program.* IA functions are defined in chapters 3 and 4 of the DoD 8570.1-M. Contractor personnel performing IA functions on this contract shall be certified at the appropriate IAT Level as demonstrated by obtaining and maintaining one (1) of the DoD approved certifications posted on the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) website (http://iase.disa.mil/eta/iawip/). The website provides a list of approved certifications for personnel performing IA functions that meet baseline IA certification requirements. Contractors may obtain any of the approved certifications to meet the applicable certification requirements for each associated level.

2. **COMPUTING ENVIRONMENT (CE) TRAINING:**
In addition to DoD IA baseline certification requirements, Contractor personnel shall obtain appropriate Computing Environment (CE) certifications for the operating system(s) and/or security related tools/devices being supported under this contract. Contractor personnel should obtain CE certifications for all tools, systems and devices being supported; however, at a minimum, Contractor personnel shall obtain a certification in the functional area(s) they spend the most time supporting (i.e. Windows7 certification for Desktops/End User Support, Cisco/ Enterasys certification for Networking, Windows 2008 for System Administration). See the DLA approved list of CE certifications in Table 2.4.1, *IAT and CE Requirements*. The approved CE list will be periodically updated to ensure relevant or expired industry standard certifications are added or removed as applicable to the CE or as directed by DoD policy. At the time of proposal submission, the Contractor shall identify personnel performing IA functions identified in the PWS prior to that employee commencing any work under this PWS and provide documentation to the KO or COR showing the employee's certification(s) and certification status. The Contractor shall demonstrate that they have a process to track certification status of employees to ensure certifications are kept current. The contractor shall replace departing employees with employees possessing current certifications in a manner that will not cause program interruption. Contractor personnel shall be required to sign the User Access Agreement, Privileged Rules of Behavior, and General Rules of Behavior and non-Disclosure agreement prior to working on any government system(s).

3. **EQUIPMENT OPERATION.** This training is required for all Contractor employees who operate motorized vehicles, MHE, other equipment with the required licensing, certification, or specialized training. Training includes but is not limited to the requirements identified in CFR Title 29, Part 1910.178; CFR Title 49; American Society of Mechanical Engineers (ASME) B30.13-1996, Storage/Retrieval (S/R) Machines and Associated Equipment; and DLAI 4500.36, Management, Acquisition, and Use of DLA Operating Equipment, Sections E3m and E3n; and Federal, State and Local Laws. Refresher training is required at a minimum of every three years or when warranted in accordance with OSHA, DoD, and manufacturer's guidance.

4. **SECURITY TRAINING**. To ensure that all Contractor employees know and understand regulations and policy pertaining to physical, information, operations and personnel security, the Contractor shall provide security and antiterrorism training to all employees in accordance with applicable DOD regulatory requirements. At a minimum, security training requirements as

required by the DLA Issuances and other applicable DOD guidance will be completed annually for: Antiterrorism/Force Protection (AT/FP), Operations Security (OPSEC), Counterintelligence Awareness Training, Information Security (INFOSEC), DoD Information Assurance Awareness and Combating Trafficking in Persons (CTIP). The security training is web-based and access will be provided by the Government. The Contractor shall ensure Contractor personnel have taken the required security training to meet DoD guidance and that the personnel continue to maintain their certifications.

5.2 CONTRACTOR FURNISHED EQUIPMENT

A. The Contractor shall provide equipment (not designated as Government furnished) which may be required for Contractor personnel to perform the requirements of this contract. The Contractor shall be responsible for all costs associated with this equipment.

1. The Contractor shall provide safety equipment while performing hazardous duties in both the office and warehouse environments. The required safety equipment may include, but is not limited to, safety shoes, glasses, harness, and equipment lanyards.

2. The Contractor shall furnish motor vehicles needed in performance of this PWS for the transportation of Contractor personnel and Government equipment to various buildings within the designated location(s). The equipment to be transported may include, but is not limited to: computers, printers, switches, tools and other miscellaneous IT hardware. The Contractor vehicle shall display the "Company Name" on the front driver and passenger door. Contractor personnel privately-owned vehicles (POVs) shall not be used for the transportation of Government-owned IT equipment. Contractor-furnished vehicles and operators shall meet all applicable licensing, insurance, registration and safety requirements.

SECTION 6 SPECIFIC TASKS

6.1 END USER (DESKTOP HARDWARE/SOFTWARE) SUPPORT REQUIREMENTS

A. The Contractor shall:

1. Provide hardware/software installation, updates, configuration, troubleshooting and resolution.

2. Provide diagnostic assistance at all levels to users of automation to determine the cause and resolution of problems encountered in the use of hardware and software. Refer, escalate and report unresolved problems and outages to enterprise technical support teams for assistance as required.

3. Provide support for all IT equipment, to include network servers, PCs, printers, scanners, portable computers, switches, routers, Blackberry devices, Multi-Functional Devices (MFDs), desktop video systems/video teleconference and projection systems that are hooked to a laptop or PC, docking stations and any external peripherals (e.g. CDROM-R/DVD, CDROM-RW, CAC readers, etc.), wireless equipment, and other miscellaneous IT equipment. Equipment is located throughout multiple buildings.

4. Manage and perform equipment relocation, installation, expansion, connection / disconnection, upgrades, support/maintenance, and preventive maintenance of computer systems hardware, documentation, and peripheral devices, to include surveying new installations and moving IT

equipment as requested; provide support to include servicing peripherals, such as printers and update associated equipment Asset Management records in accordance with policy.

5. Test and install computer hardware and software applications and ensure software applications meet end user requirements, and compliance to DLA's Computer Emergency Response Team (CERTs) and Security Technical Implementation Guide (STIG) mandates.

6. Plan and coordinate the removal, movement, and/or installation of computer hardware and software to include updating Asset Management System.

7. Provide support for CAC (Common Access Card) deployment. Install smart card readers, middleware, and PKI (Public Key Infrastructure) Certificates. Provide troubleshooting, guidance and training to DLA personnel on use of the CAC card and its software certificates.

8. Provide on-site service for multiple divisions and other remote customers on an as required basis. IT support shall be required for disconnection, connection, installation, or relocation of PCs and associated peripherals. Guidance shall be provided for new equipment installations according to DLA Information Operations standard specifications.

9. Printer maintenance:
   (a) Install and maintain all types of network and PC attached printers (bar code, pRFID, & laser).
   (b) Install and configure network print servers.
   (c) Troubleshoot problems with print servers.

10. Excess IT Equipment:
   (a) Deliver unserviceable or excess IT equipment to staging area for disposal.
   (b) Prepare hard drives for disposal in accordance with policy and provide records to the Technical Point of Contact (TPOC).
   (c) Complete and provide documentation to the Accountable Property Officer (APO) to adjust inventory for any relocation or disposal of IT equipment.

11. Software Support:
   (a) Provide software support to include any subsequent releases/upgrades/patches, configuration, troubleshooting and resolution for various commercial software packages.
   (b) Provide software integration, identification of products to meet customer's requirements current and future.
   (c) Provide technical support on software installation and configuration.
   (d) Utilize approved automated systems and processes to remotely deploy all applicable software upgrades, patches, and mandated Computer Emergency Response Team (CERT) taskings.
   (e) Maintain and update IT inventory in accordance with the DLA Information Operations at New Cumberland Instruction Number 4200.01 Information Technology Asset Management, including Accountable Property Standard Operating Procedures for control and location of IT assets.
   (f) Provide support and/or troubleshooting for applications to include, but not limited to:
      - Microsoft Windows
      - Microsoft Office
      - Microsoft Active Directory (AD)
      - COTS applications (i.e. WebSphere, Globe Ranger)

- Depot-unique applications (i.e. DISA's Multi-Host Internet Access Portal (MIAP), Distribution Standard System (DSS), Equipment Control System (ECS), etc.)

12. Contact proper vendor repair personnel for warranty repairs or when proprietary repairs are required. Explain and demonstrate malfunctions to equipment vendors responding to warranty calls or proprietary contractor calls. Verify that vendors who are servicing warranties or making proprietary repairs made proper repairs.

6.2 NETWORK ADMINISTRATION SUPPORT REQUIREMENTS

A. The Contractor shall:

1. Monitor various systems' performance, troubleshoot system problems, and conduct technical diagnostic analysis to determine the source of the hardware and/or system problem and develop data recovery methods if necessary. Refer, escalate and report unresolved problems and outages to enterprise technical support teams for assistance as required.

2. Develop and provide support services, including instructions, guidance, and training relative to the use of installed application database software systems.

3. Implement applicable patches including Information Assurance Vulnerability Assessments (IAVAs), Information Assurance Vulnerability Bulletin (IAVBs), and Taskings (TAs) for their network environment (NE).

4. Apply security requirements to the operating system for the network environment (NE) and computing environment (CE) used in their current position.

5. Configure and administer Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS), Windows Internet Naming Service (WINS), and Transmission Control Protocol/Internet Protocol (TCP/IP) network support.

6. Receive, process, and report final response/actions for Computer Emergency Response Team (CERT) Taskings and IAVAs to curtail vulnerabilities.

7. Search computer and network logs for unauthorized entry attempts or activity and reporting any findings.

8. Information Assurance (IA) Functions:
   (a) Examine potential security violations to determine if the NE has been breached, assess the impact, and preserve the evidence.
   (b) Support, monitor, test, and, troubleshoot hardware and software IA problems pertaining to the NE.
   (c) Recommend and schedule IA-related repairs in the NE.
   (d) Manage accounts, networks rights, and access to the NE systems and equipment.
   (e) Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
   (f) Perform system audits to assess security related factors within the NE.

9. Maintain the network from the routers to end-user workstations.

10. Troubleshoot network routers, hubs, smart switches, interior cable infrastructure, replacing and repairing as required.

11. Radio Frequency (RF) Support/Service:
    (a) Determine the location, installation and cabling requirements for access points and antennas.
    (b) Troubleshoot problems with RF terminals, Smart-Cart system (RF bridge unit, Inverter, Charger, batteries, PC, monitor, printer(s)), and RF network service for buildings.
    (c) Determine optimum configuration for RF Base — RF Bridge and configure the units.
    (d) Troubleshoot problems with the RF Base — RF Bridge network for 2.4 GHz or later frequencies.
    (e) Perform troubleshooting normally associated with network-connected terminals for software and hardware problems.
    (f) Program RF devices and controllers units using Standard Operating Procedures (SOP) instructions provided.
    (g) Use provided man-lift or approved/inspected ladders for the installation of access points, antenna and cabling required for established service and to retrieve defective units for repair.
    (h) Provide support in accordance with the DLA Information Operations Wireless Policy (refer to Attachment 5.3, *DoD Wireless Instructions, 8420.01*).

12. Provide Software Support:
    (a) Provide software support to include any subsequent releases/upgrades/patches, configuration, troubleshooting and resolution for various commercial software packages.
    (b) Provide software integration, identification of products to meet customer's requirements current and future.
    (c) Provide technical support on software installation and configuration.
    (d) Utilize approved automated systems to remotely deploy all applicable software upgrades, patches, and mandated CERTs.
    (e) Maintain IT inventory in accordance with the DLA Information Operations at New Cumberland Instruction Number 4200.01 Information Technology Asset Management, including Accountable Property Standard Operating Procedures.
    (f) Provide software support to include but not limited to the following:
        - Distributed Sniffer software suite
        - Switch/Router management software suite
        - Vulnerability Scanning software suite
        - DLA COTS applications (i.e. WebSphere, Globe Ranger)
        - Depot-unique applications

6.3 PROPERTY ACCOUNTABILITY

A. The Contractor shall maintain care of all Government-furnished property. At all times during the performance of the contract requirements, title to the mission stock and all other government-furnished property shall remain vested with the Government. In exercising care and custody, the Contractor shall safeguard all Government-furnished property.

B. The Contractor shall provide the proper protection for material under their custody and control. If there is a loss the Contractor shall immediately notify the KO or COR.

6.3.1 LIABILITY FOR GOVERNMENT PROPERTY

A. The Contractor shall be held financially liable for loss, damage, or destruction of government property caused by negligence, willful misconduct or unauthorized use. The KO or COR will make the pecuniary liability determination when a Contractor's negligence results in loss, damage, or destruction of Government property.

B. The Contractor shall:

1. Notify the KO or COR immediately when it discovers the gain, loss, damage or destruction of government equipment or property.
2. Conduct an initial search and/or informal investigation into the loss or damage of equipment or property and forward all research data to the KO or COR.
3. Cooperate in any subsequent investigations.

6.3.2 INDEMNIFICATION AND LIMITATION OF LIABILITY

A. The Contractor shall indemnify the Government and hold it harmless against claims for injury to persons or damage to property of the Contractor or others arising from the Contractor's possession or use of the government facilities, from its activities, or from its use, care and custody of the mission stock and government equipment and supplies relating to the performance of this contract.

B. When the KO or COR determines that any loss, damage or destruction of mission stock or other government property is caused by the Contractor's negligence, willful misconduct or unauthorized use, the KO or COR may off-set payments under the contract by the determined value of the loss, damage or destruction. The Contractor's liability per occurrence shall be limited to $50,000 with a total limit of liability of $1,000,000 per year. This limit of liability does not apply to the Government's right to indemnification.

6.4 RECORDKEEPING

A. The Contractor shall utilize the Employee Activity Guide for Labor Entry (EAGLE) IT system which is DLA's designated Time and Project Tracking System to input consolidated time spent on tasks performed using predetermined codes provided within the tracking system.

B. The Contractor shall utilize the Incident and Asset Management Tracking System to identify, schedule, document and complete all trouble call actions and requests.

C. All documentation, record and databases, as described in this PWS, are the property of the Government. All files developed in performance of the work under this contract are the property of the Government. The Contractor shall turn all files over to the KO or COR at the completion or termination of this contract.

6.5 SECTION 508 COMPLIANCE REQUIREMENTS

Section 508 must be considered as a requirement on the delivered content to assure that it includes data and/or knowledge appropriate to specific Section 508 accessibility requirements. Solicitation respondents must describe how their experience and skills will result in Electronic and Information Technology (EIT) deliverables meet at least those technical provisions identified as applicable in the attached Government

Product/Service Accessibility Template (GPAT), Software Development Services. The standards in the DDNV Support GPAT define the types of technology covered and set forth provisions that establish a minimum level of accessibility. Only proposals which contain adequate information to document their responsiveness to the Section 508 requirements (e.g. a completed GPAT, VPAT or equivalent and supporting documentation) shall be considered.

6.6 QUALITY CONTROL PLAN

A. DLA is committed to a highly interactive relationship between quality control by the Contractor and quality assurance by the government recipient of services. This relationship shall be achieved through a Prevention Based Quality System dedicated to ensuring the best possible products and services to DLA end users. The Contractor shall provide their final QCP no later than (NLT) 10 calendar days after the start of full performance in accordance with paragraph 6.5B.

B. The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance (e.g., all functional areas, all Acceptable Performance Level (APL) and non-APL requirements). The QCP shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the contract. Within 24 hours of completion, the Contractor shall provide to the KO or COR, all reports generated as a result of the Contractor's quality control efforts. This shall include any summary information used to track quality control, including any charts/graphs.

C. The Contractor's QCP shall be incorporated into and become part of this contract after the plan has been accepted by the Government. Changes made after KO or COR approval shall be submitted in writing to the KO or COR for review and acceptance. The Contractor's QCP shall be maintained throughout the life of the contract and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the contract.

D. DLA Information Operations will implement a Quality Assurance Surveillance Plan (QASP) to ensure the contractor provides the required services and adheres to quality standards as specified in this PWS. The KO or COR shall monitor performance. This monitoring by the KO or COR shall be carried out via the QASP as identified in the attachment to this PWS entitled, "Quality Assurance Surveillance Plan (QASP) for IT Support Services. This QASP document shall also ensure the Contractor's QCP effectiveness and provides a systematic method to evaluate the services the Contractor is required to furnish.

6.7 DELIVERABLES

A. The Contractor shall submit the following deliverables:

6.7.1 TASK ACTIVITY TRACKING

A. The Contractor shall input into EAGLE consolidated time spent on tasks performed using predetermined codes within the tracking system.

6.7.2 WORK ORDER/INCIDENT TICKET TRACKING

A. The Contractor shall utilize the designated Incident and Asset Management Tracking System to identify, schedule, and complete all trouble call actions and requests.

B. Within 24 hours after completion of a work order, the Contractor shall input into the Incident and Asset Management Tracking System completed incident documentation.

6.7.3 WEEKLY STATUS REPORTS

A. The Contractor shall provide a weekly report that identifies work completed for the specified time period, any issues that could not be resolved, and any suspense that could not be met with an explanation for the delay.

6.7.4 CONFIGURATION MANAGEMENT

A. The Contractor shall provide documentation of installations/upgrades, to include screenshots, diagrams, technical specifications, and guidance for future reference.

B. The Contractor shall provide all required certifications of personnel performing work under this contract in accordance with the specifications identified for each certification in this PWS (i.e. IA, MHE, etc.).